REMARKS

Applicants thank the Examiner for his time during the telephonic interview of July 10, 2006. We discussed at length the cited references and claim rejections as set forth in the Office Action, and the Examiner requested that Applicants submit the points discussed in this formal Response. Applicants look forward to the Examiner's response to this paper, and respectfully invite the Examiner to contact Applicants' representatives at any time to discuss this application if the Examiner determines that these claims are not in condition for allowance (particularly in view of the lengthy period of prosecution of this application thus far).

In the Office Action, claims 1-13, 17-29, 33-45, 49 and 50 are rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over U.S. Patent No. 5,263,162 to Bush *et al.* (hereinafter "Bush") in view of U.S. Patent No. 6,484,260 to Scott *et al.* (hereinafter "Scott"). The remaining claims are rejected as inherent in view of Bush.

Bush is directed to a portable PIN card that dynamically generates for each transaction an encrypted PIN from the combination of a user entered PIN and a pseudo-random number computed by a central computer. (*See* Bush, Abstract). The encrypted PIN is then transmitted to the central computer for authorization. (*Id.*). As conceded by the Examiner, Bush does not teach a system for transmitting a non-ATM PIN to be entered by a user in a transaction (*See* Office Action, p. 3). Additionally, the Examiner has previously conceded that Bush does not teach the entry of a non-ATM electronic commerce PIN by the user (*See* previous Office Action, p. 2).

However, the Examiner alleges that Scott discloses an inventive concept where a non-electronic commerce PIN is to be entered by the user (*See* Office Action, p. 3, *citing* Scott, col. 11, ln. 45 - col 12, ln. 6). Scott is directed to a personal identification device ("PID") for

providing secure access to a host facility using biometric data supplied by a user. Abstract. A processing unit located on the PID compares the biometric signal supplied by the user to stored biometric data in order to authenticate the user. A verification signal is provided only if the supplied biometric data corresponds sufficiently to the stored biometric data. A communication unit, also located on the PID, is adapted to transmit a verification signal to the host system upon authentication. Thus, the system of Scott allows a user to utilize the combination of the PID and biometric data (such as a fingerprint) in lieu of a bank card and PIN to access an ATM.

Applicants submit that Scott does not disclose or suggest entering a non-electronic commerce PIN in a second transaction type as is required by claim 1. First, Applicants submit that the biometric data entered by the user in Scott cannot be considered a non-electronic commerce PIN because (a) it is not a number (i.e., Personal Identification Number) and (b) it is not entered by the user. Rather, the biometric data is unique for each user and is unalterable.

Additionally, the biometric data supplied by the user in Scott is not related to the ATM PIN in any manner. In contrast, the non-electronic commerce PIN in Applicants' invention is generated directly from the ATM PIN using a cryptographic operation.

Moreover, even if the biometric data of Scott could be considered a non-electronic commerce PIN, it is only used as an alternative means of accessing an ATM (in lieu of a bank card and PIN). Therefore, it cannot be considered as being used in a second transaction type that is a non-ATM financial transaction as is required by, e.g., claim 1 of the present application.

Furthermore, Scott does not disclose the additional claim limitation of transmitting said non-ATM electronic commerce PIN to said user. In contrast, Scott teaches away from

this claim limitation since the biometric data comes directly from the user and is not generated on a central computer (as is required in Applicants' invention). Indeed, there is no reason for the system of Scott to transmit any data to the user, as even the electronic identification information stored in the device is transmitted transparently from the user – the user of the Scott system knows only that he or she needs to give thumbprint information. Therefore, there is no need to transmit any information, including a non-ATM electronic commerce PIN, to the user. Alternatively, the transmission of the e-commerce PIN to the user is critical, so that the user may enter the e-commerce PIN to complete, *e.g.*, later transactions over the Internet, using that e-commerce PIN.

Notwithstanding the above noted remarks, Applicants incorporate fully, and reiterate herein, the arguments set forth in Applicants' Response to Office Action dated February 2, 2006.

In contrast to the cited prior art, the present invention is directed to, *inter alia*, a method for generating identification data wherein a central computer cryptographically generates a non-ATM electronic commerce PIN derived from a user PIN. The non-ATM electronic commerce PIN is then transmitted to the user for later use in non-ATM financial transactions. When the user proceeds to execute a non-ATM electronic transaction (e.g., a transaction via the Internet), instead of inserting a PIN, the user enters the non-ATM electronic commerce PIN that was generated by the central computer.

Further, Applicants respectfully assert that Bush differs materially from the claims as amended. For example, in Bush for each and every transaction, the *card* dynamically generates an encrypted, randomized PIN that differs from the encrypted PIN used in the previous transaction. In the system of Bush, the user does not have to remember the generated PIN (indeed, as a practical matter, the user cannot, since a new PIN is generated

for every transaction in Bush), nor does the user ever have to enter this generated PIN to complete a transaction. In the present invention as amended, on the other hand, not only does the *central computer* generate the non-ATM electronic commerce PIN, the non-ATM electronic commerce PIN generated by the central computer is intended to be memorized by the user and used *multiple times*.

Further, as conceded by the Examiner and as described above, Bush does not disclose a system for transmitting a non-ATM PIN to be entered by a user in a transaction. Rather, Bush discloses entry of only an unencrypted PIN into the card. However, the presently claimed invention requires the entry of a non-ATM electronic commerce PIN, which is, in effect, an encrypted PIN.

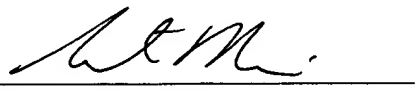
Finally, because the encrypted PIN is generated on the card, Bush clearly does not disclose a central computer transmitting a non-ATM electronic commerce PIN to the user.

For these reasons, Applicants respectfully assert that the amended claims are now in condition for allowance.

CONCLUSION

In view of the foregoing, Applicants respectfully submit that claims 1-13, 17-29, 33-45, 49 and 50 (all of the pending claims) are in condition for allowance. In the event that the application is not deemed in condition for allowance, the Examiner is invited to contact the undersigned in an effort to advance the prosecution of this application.

Respectfully submitted,



Robert C. Scheinfeld
Patent Office Reg. No. 31,300
(212) 408-2512

Robert L. Maier
Patent Office Reg. No. 54,291
(212) 408-2538

Attorneys for Applicants

BAKER BOTTS, L.L.P.
30 Rockefeller Plaza
New York, New York 10112-4498